

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

ALEXANDER KONSTANTINOVICH  
TVERDOKHLEBOV,

Defendant.

CRIMINAL NO.: 1:17-CR-9

**STATEMENT OF FACTS**

The United States and ALEXANDER TVERDOKHLEBOV (“Defendant” or “TVERDOKHLEBOV”) agree that the following facts are true and correct, and that had this matter proceeded to trial, the United States would have proven beyond a reasonable doubt with admissible and credible evidence that from on or about May 2008 through at least on or about February 2010, the Defendant, having devised a scheme or artifice to defraud and for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, such scheme affecting financial institutions, transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice. At all relevant times, the Defendant acted with the intent to defraud.

The United States and the Defendant further agree that the evidence at trial would establish, at a minimum, the following facts:

1. TVERDOKHLEBOV resided in the United States from at least 2007 until the present.

2. From at least 2008 until the present, TVERDOKHLOBOV was an active member of several elite Russian-speaking cybercrime forums. The purpose of the forums is to facilitate cybercrimes, help cybercriminals find co-conspirators, and promote the buying and selling of illegal services such as money laundering and computer intrusions services, and the buying and selling of illegal goods such as stolen credit card information and personal identifying information (PII). Membership in the most elite forums of which TVERDOKHLOBOV was a member was restricted to Russian-speaking cybercriminals who could prove their criminal bonafides by finding current members to “vouch” for them.

3. To accomplish the fraudulent scheme alleged in the indictment, TVERDOKHLOBOV worked with a Russian national named V.P. Until his extradition to the United States in 2015, V.P. resided outside the United States.

4. “ICQ” was a brand of software used for instant chat messaging. From at least 2008 through at least 2010, ICQ transmitted and received all communications between its users through servers located in Dulles, Virginia, as well as other locations, within the Eastern District of Virginia.

5. The term “botnet” refers to a group of computers (known as “bots”) that have been infected with malicious software that typically allows the operator of the botnet to covertly access the bots and steal information, such as online banking passwords and login credentials. Botnet operators frequently use the stolen information to commit fraud, or to sell to others who intend to use the information to commit fraud.

6. From on or about May 2008 through on or about February 2010, TVERDOKHLEBOV used ICQ to communicate with V.P. for the purposes of devising and executing a scheme to defraud. In particular, TVERDOKHLEBOV devised a scheme to defraud

whereby he used a botnet and similar methods of unlawful computer intrusions, to steal passwords and login credentials for online banking accounts. As part of the scheme, TVERDOKHLEBOV, and accomplices such as V.P., would then use the stolen passwords and login credentials to make fraudulent purchases and/or fraudulent withdrawals from the victim's online banking accounts. As part of the scheme to defraud, TVERDOKHLEBOV possessed and trafficked in over 40,000 unauthorized access devices, specifically stolen credit card numbers, that TVERDOKHLEBOV intended to use or allow others to use to for the purpose of fraudulent transactions. As part of the scheme to defraud, TVERDOKHLEBOV controlled and operated botnets of over 500,000 infected computers from which TVERDOKHLEBOV intended to extract sensitive financial information.

7. As stated in paragraph 4 above, each ICQ message between TVERDOKHLEBOV and V.P. caused a wire communication to be transmitted into and out of servers located in the Eastern District of Virginia.

8. In furtherance of the scheme described above, the following acts were committed in the Eastern District of Virginia and elsewhere:

a. On or about the dates set forth below, in the Eastern District of Virginia and elsewhere, the defendant, ALEXANDER TVERDOKHLEBOV, having devised and intending to devise a scheme or artifice to defraud, and for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, namely, the fraudulent scheme described in paragraph 7 above, transmitted and caused to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme or artifice. At all times, the scheme described in this paragraph and

paragraph 7 above affected a financial institution, as used in 18 U.S.C. § 1343 and defined in 18 U.S.C. § 20.

b. In particular, TVERDOKHLEBOV sent the following wire transmissions, via the instant messaging service ICQ, to his accomplice V.P. for the purpose of executing the scheme described above. Each message was transmitted into and out of servers located in the Eastern District of Virginia.

Date	Description of Wire Transmissions
10/28/2008	TVERDOKHLEBOV sent ICQ messages to V.P. providing V.P. with stolen online banking passwords and login credentials and asking for assistance in making fraudulent transfers of funds from the compromised account.
10/29/2008	TVERDOKHLEBOV sent ICQ messages to V.P. discussing how they could use a botnet to steal online banking passwords and login credentials for the purpose of engaging in fraudulent transactions.
11/15/2008	TVERDOKHLEBOV sent ICQ messages to V.P. discussing which method should be used to mine stolen data to find the victims' online banking passwords and login credentials.
11/17/2008	TVERDOKHLEBOV sent ICQ messages to V.P. telling him how to access banking passwords and login credentials that had been stolen through their botnet and directing V.P. to make fraudulent purchases using these stolen passwords and credentials.

9. In connection with his scheme to defraud, TVERDOKHLEBOV made the following representations on several of the elite cybercrime forums restricted to Russian-speaking cybercriminals:

- a. That he possessed 40,000 stolen credit card numbers and was soliciting buyers for the stolen information (post on cybercrime forum dated November 14, 2009).
- b. That he had control of or operated a botnet with 10,000 bots and that cybercriminals could contact him to rent this botnet (private message between TVERDOKHLEBOV and another member of a cybercrime forum dated June 3, 2009).

- c. That he had control of or operated a botnet with 300,000 bots and that cybercriminals could contact him to rent this botnet (private message between TVERDOKHLEBOV and another member of a cybercrime forum dated June 21, 2012).
- d. That he had control of or operated a botnet with 500,000 bots and that cybercriminals could contact him to rent this botnet (post on cybercrime forum dated January 15, 2013).
- e. That he possessed an unknown quantity of “dumps,” which is a word used to describe stolen credit card information, which he was willing to sell to other cybercriminals in increments of 1,000 stolen or fraudulently obtained credit card numbers of victims order to extract cash, and in which the “validity” of these “dumps” was 90%, meaning that 90% of these credit card numbers were active, and thus could be used to extract funds (post on cybercrime forum dated October 30, 2013).
- f. That he possessed an unknown quantity of dumps, which he was willing to sell to other cybercriminals in increments of 1,000 stolen or fraudulently obtained credit card numbers, and in which the “validity” of these “dumps” was 85%, meaning that 85% of these credit card numbers were active, and thus could be used to extract funds (post on cybercrime forum dated August 3, 2014).
- g. That he possessed “dumps” and “pins,” and would be willing to work with other cybercriminals in order to “cash out” the accounts corresponding to the

stolen or fraudulently obtained financial information (post on cybercrime forum dated May 27, 2010).

10. In connection to his scheme to defraud, TVERDOKHLEBOV worked with two Russian students who were living in the United States in 2008 to fraudulently obtain funds from a compromised bank account, some of the proceeds of which were sent to TVERDOKHLEBOV. A loss of approximately \$77,000 is attributable to this part of the scheme.

11. In connection to his scheme to defraud, TVERDOKHLEBOV used a botnet to obtain sensitive financial information from at least 100 victims from 2010 through 2015. Some of this information included the PayPal account information of at least one victim residing in the Eastern District of Virginia.

12. TVERDOKHLEBOV earned over a million dollars of criminal proceeds from the illegal schemes described in this statement of facts. At the time of his arrest on February 1, 2017, TVERDOKHLEBOV stored \$272,000 in criminal proceeds in cash in four safe-deposit boxes located in Los Angeles, California and Las Vegas, Nevada. Additionally, TVERDOKHLEBOV stored additional criminal proceeds in several bank accounts located in the United States and abroad and in a virtual currency called Bitcoin.

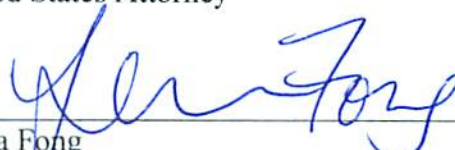
13. The statement of facts includes those facts necessary to support the Defendant's guilty plea. It does not include each and every fact known to the Defendant or to the government and it is not intended to be a full enumeration of all of the facts surrounding the Defendant's case.

14. The actions of the Defendant, as recounted above, were in all respects knowing, voluntary, and intentional, and were not committed by mistake, accident or other innocent reason. At all relevant times, the Defendant acted with the intent to defraud.

15. The Defendant waives any rights under Fed. R. Crim. P. 11(f), Fed. R. Evid. 410, the United States Constitution, and any federal statute or rule in objecting to the admissibility of the Statement of Facts in any such proceeding.

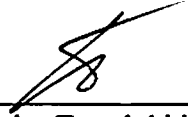
Dana J. Boente  
United States Attorney

By: \_\_\_\_\_

  
Laura Fong  
Kellen S. Dwyer  
Assistant United States Attorneys

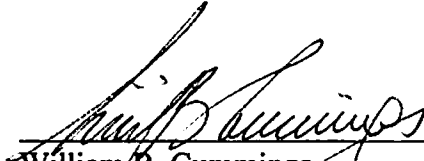
**Defendant's Signature:** I hereby agree that I have consulted with my attorney and fully understand all rights with respect to the pending criminal indictment. Further, I fully understand all rights with respect to Title 18, United States Code, Section 3553 and the provisions of the Sentencing Guidelines Manual that may apply in my case. I have read this plea agreement and carefully reviewed every part of it with my attorney. I understand this agreement and voluntarily agree to it.

Date: 03/16/17

  
\_\_\_\_\_  
Alexander Tverdokhlebov  
Defendant

**Defense Counsel Signature:** I am counsel for Alexander Tverdokhlebov. I have fully explained to the defendant the defendant's rights with respect to the pending indictment. Further, I have reviewed Title 18, United States Code, Section 3553 and the Sentencing Guidelines Manual, and I have fully explained to the defendant the provisions that may apply in this case. I have carefully reviewed every part of this plea agreement with the defendant. To my knowledge, the defendant's decision to enter into this agreement is an informed and voluntary one.

Date: 3-16-17

  
\_\_\_\_\_  
William B. Cummings  
Counsel for the Defendant